ارقمات
2018/5/17
المحاضرة ...

الموضوع: محاضرة 8 نظري

دالة أويلر: هي الدالة التي تقارن لكل عدد طبيعي n بعدد $\varphi(n)$

$$n \longrightarrow \varphi(n) = |U(Z_n)| = Z_n^*$$

$U(Z_n) = \{a \in Z_n : d(a,n) = 1\}$ ⇐ $Z_n = \{0,1,2,3,\dots,n\}$

$U(Z_{16}) = \{1,3,5,7,9,11,13,15\}$

مبرهنة اولى: إذا كان a عدد صحيح و n عدد طبيعي بحيث أوليان فيما بينهما $d(a,n)=1$ عندئذٍ:

$$a^{\varphi(n)} \equiv 1 (mod\ n)$$

الإثبات: $(Z_n, +, \cdot)$ حلقة، زمرة الضربية هي

$$U(Z_n) = \{\bar{a} \in Z_n : d(a,n) = 1\}$$

$$\bar{a} \in U(Z_n) \Leftarrow d(a,n) = 1$$

ومنه حسب مبرهنة لاغرانج ونتائجها يكون:

$$(\bar{a})^{|U(Z_n)|} = \bar{1}$$

> مبرهنة لاغرانج
> $|G| = m$
> $x \in G : x^m = e$
> محايد عنصر الزمرة

ومنه

$$(\bar{a})^{\varphi(n)} = \bar{1} \Rightarrow \overline{a^{\varphi(n)}} = \bar{1}$$

$$\Leftrightarrow a^{\varphi(n)} \equiv 1 (mod\ n)$$

وهو المطلوب.

> بالقياس n
> $\bar{x} = \bar{1} \Leftarrow x \equiv$

نتيجة: إن مبرهنة فيرما حالة خاصة من أويلر

$a^{p-1} \equiv 1 (mod\ p)$ فإن $p \nmid a$

بالعكس: $p \nmid a$

$$p \nmid a \Rightarrow d(p,a) = 1$$

$$\varphi(p) = p - 1$$

وحسب ما سبق:

ومنه حسب أويلر:

$$a^{p-1} \equiv 1 (mod\ p)$$

مبرهنة ②: $n = p^{\alpha}$ حيث p عدد أولي و α عدد صحيح موجب $(\alpha \in Z^+)$

فإن:

$$\varphi(p^{\alpha}) = p^{\alpha} - p^{\alpha-1} = p^{\alpha}\left(1 - \frac{1}{p}\right)$$

$$= p^{\alpha-1}(p-1)$$

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

② العبارة القانونية

مثال ١

$$\varphi(n) = n \cdot \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right) = \frac{n \prod_{i=1}^{k} (p_i - 1)}{\prod_{i=1}^{k} p_i}$$

. الإثبات: وجدنا φ دالة ضربية (نتقبلها دون برهان)

. وبما أن $p_1, p_2 \cdots p_k$ أعداد مختلفة فهي نسبية أولياً فإن كل منها ومن ثم الأولية $p_1^{\alpha_1}, p_2^{\alpha_2}, \cdots p_k^{\alpha_k}$ نسبياً مثنى مثنى، وبالتالي:

$$\varphi(n) = \varphi(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k})$$

$$= \varphi(p_1^{\alpha_1}) \cdot \varphi(p_2^{\alpha_2}) \cdots \varphi(p_k^{\alpha_k})$$

$$= p_1^{\alpha_1}\left(1 - \frac{1}{p_1}\right) \cdot p_2^{\alpha_2}\left(1 - \frac{1}{p_2}\right) \cdots p_k^{\alpha_k}\left(1 - \frac{1}{p_k}\right)$$

$$= n\left(\frac{p_1 - 1}{p_1}\right)\left(\frac{p_2 - 1}{p_2}\right) \cdots \left(\frac{p_k - 1}{p_k}\right)$$

$$= p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right)$$

$$= \frac{n \prod_{i=1}^{k} (p_i - 1)}{p_1 \cdot p_2 \cdots p_k} = n \prod_{1}^{k}\left(1 - \frac{1}{p_i}\right)$$

. مثال احسب $\varphi(360)$

360	2
180	2
90	2
45	3
15	3
5	5
1	

$$360 = 2^3 \cdot 2^2 \cdot 5$$

$$\varphi(360) = 360\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right)$$

$$= 360\left(\frac{1}{2}\right)\left(\frac{2}{3}\right)\left(\frac{4}{5}\right)$$

$$= 96$$

$$\mathbb{Z}_{360} = \{0, 1, 2, \cdots, 359\}$$

$$|U(\mathbb{Z}_{360})| = 96 = \varphi(360)$$

[illegible] مع 360

$$U(\mathbb{Z}_{360}) = \{a \in \mathbb{Z}_{360} : d(a, 360) = 1\}$$

الموضوع:

بعض التمارين البسيطة:

تمرين: أوجد رقمي الآحاد والعشرات (أي العدد المكون من الآحاد والعشرات) للعدد 3^{256}

(رقم الآحاد: باقي قسمة العدد على 10 — رقم العشرات: باقي قسمة العدد على 100)

العدد المطلوب المكون من آحاد وعشرات هو باقي قسمة هذا العدد على 100

$$3^{256} \equiv k \pmod{100}$$

الحل: نلاحظ أن $d(3,100)=1$ حسب أويلر:

$$3^{\varphi(100)} \equiv 1 \pmod{100}$$

ولكن

$$\varphi(100) = \varphi(2^2 \cdot 5^2)$$

(حسب تحليل العدد لعوامله الأولية $4 \cdot 25$)

$$= 100\left(1-\tfrac{1}{2}\right)\left(1-\tfrac{1}{5}\right)$$

$$= 100\left(\tfrac{1}{2}\right)\left(\tfrac{4}{5}\right) = 40$$

(إذا كان العدد بالـ (3) أكبر المضاعف نقسمه على المضاعف ونأخذ ناتج القسمة)

$$256 = 6 \cdot 40 + 16$$

$$3^{256} = (3^{40})^6 \cdot 3^{16} \equiv 1^6 \cdot 3^{16} \pmod{100}$$

$$= (3^4)^4 \pmod{100} \equiv (81)^4 \pmod{100}$$

($81 + 19 = 100$)

$$\equiv (-19)^4 \pmod{100}$$

$$\equiv [(-19)^2]^2 \pmod{100}$$

$$\equiv (361)^2 \pmod{100}$$

$$\equiv (61)^2 \pmod{100}$$

($361 = 3 \cdot 100 + 61$)

$$\equiv (-39)^2 \pmod{100}$$

$$\equiv (1521) \pmod{100}$$

$$\equiv (15 \cdot 100 + 21) \pmod{100}$$

$$\equiv 21 \pmod{100}$$

أي أن باقي قسمة 3^{256} على 100 هو 21

لإيجاد $(503)^{256}$ قسم 503 ع 100 بالقسمة $\boxed{3^{256}}$

نأخذ الباقي

$503 = 5 \cdot 100 + 3$

. إذا كان الأساس أكبر من المقياس نقسم على المقياس ونأخذ الباقي ونضعه بداله أول.

ج) مثال: نفرض أن m و n عددان صحيحان موجبان أوليان فيما بينهما

$d(n,m)=1$ و $n,m \in Z^+$

. عندئذٍ أثبت أن: $[m^{\varphi(n)}+n^{\varphi(m)}]\equiv 1 (mod\ m\cdot n)$

الحل حسب أويلر

$m^{\varphi(n)} \equiv 1 (mod\ n) \Rightarrow n \mid [m^{\varphi(n)}-1]$

$n^{\varphi(m)} \equiv 1 (mod\ m) \Rightarrow m \mid [n^{\varphi(m)}-1]$

n و m أوليان وجداءهما يقسم جداء هذين العددين

$n\cdot m \mid (m^{\varphi(n)}-1)(n^{\varphi(m)}-1)$

$n\cdot m \mid [\underbrace{m^{\varphi(n)}\cdot n^{\varphi(m)}}_{a} - \underbrace{m^{\varphi(n)} - n^{\varphi(m)} + 1}_{b}]$

لدينا $m \mid m^{\varphi(n)}$ و $n \mid n^{\varphi(m)}$

وبالتالي الجداء يقسم الجداء

$n\cdot m \mid n^{\varphi(m)}\cdot m^{\varphi(n)}$

. لدينا n.m يقسم الجداء (a) و n.m يقسم الجداء كامل

. إذن:

$n\cdot m \mid [1 - m^{\varphi(n)} - n^{\varphi(m)}]$

$n\cdot m \mid [n^{\varphi(m)} + m^{\varphi(n)} - 1] \Rightarrow [n^{\varphi(m)}+m^{\varphi(n)}] \equiv 1 (mod\ n\cdot m)$.

وهو المطلوب.

مسألة (ترسيم) اثبت أن $\varphi(n)$ ، $n>2$ عدد زوجي دوماً

الحل: نفرض أن ناتج تحليل n لعوامله الأولية (العبارة القانونية) هو :

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

$$\varphi(n) = p_1^{\alpha_1 - 1} \cdot p_2^{\alpha_2 - 1} \cdots p_k^{\alpha_k - 1} \cdot (p_1 - 1)(p_2 - 1) \cdots (p_k - 1)$$

$(p_1 < p_2 < \cdots < p_k)$ زوجية دائماً

لأن p_i أولية فردية تختلف اعتباراً من $i = 2, \cdots$

وبالتالي $\varphi(n)$ سيكون عدداً زوجياً.

طريقة ثانية على مناقشة حالتين.

ⓐ $n = 2^k$ حيث $k \geq 2$ فإن (n قوة للعدد k)

$$\varphi(2^k) = 2^k - 2^{k-1}$$
$$= 2^{k-1}(2-1) = 2^{k-1}$$

وهو عدد زوجي

ب) إذا لم تكن n قوة للعدد 2 فهو يقبل القسمة على عدد أولي فردي حتماً
وليكن p يقسم n :

$s \geq 1$ و $n = m \cdot p^s$ وحيث،

$$d(p, m) = 1 \Rightarrow d(p^s, m) = 1$$

ومن ثم ولأن φ دالة ضربية يكون:

$$\varphi(n) = \varphi(m) \cdot \varphi(p^s) = \varphi(m)\, p^{s-1}\,(p-1)$$

$(p-1)$ زوجي لأن p فردي

فالناتج عدد زوجي.

تمرين: اثبت أن العدد $22 \mid [3^{10n+2} + 5^{10n+1} - 2]$

$22 = 2 \cdot 11$

اذاً الباقي 0 يقسم

الحل

$d(3,22)=1$

$3^{\varphi(22)} \equiv 1 \pmod{22} \Rightarrow 3^{10} \equiv 1 \pmod{22}$

$d(5,22)=1$

$5^{\varphi(22)} \equiv 1 \pmod{22} \Rightarrow 5^{10} \equiv 1 \pmod{22}$

$[3^{10 \cdot n+2} + 5^{10 \cdot n+3}] = [(3^{10})^n 3^2 + (5^{10})^n 5^3 - 2]$

$= [(1)^n 3^2 + (1)^n 5^3 - 2] \pmod{22}$

$\equiv 0 \pmod{22}$ ← $132 \pmod{22}$

تمرين: أثبت أن العدد n أولي إذا وفقط إذا كان:

$\varphi(n)=n-1 \iff$ n أولي

الحل: إذا كان n أولي ⟸ $\varphi(n)=n-1$

لأن جميع الأعداد الأصغر من n أولية مع n ابتداءً من (1)

فهو محقق $(n-1)$ — ①

نفرض أن $\varphi(n)=n-1$

لنثبت أن n أولي.

لو كان n غير أولي لوجد قاسم له مثل d يحقق الشرط،

$1<d<n : d|n$

أي يوجد بين مجموعة الأعداد $1,2,3,\dots n-1$

عدد واحد على الأقل ليس أولي مع n هو (d) وعندئذٍ سيكون،

$\varphi(n) \leq n-2$

وهذا يتناقض مع الفرض لأن $\varphi(n)=n-1$،

لذلك n لا يمكن أن يكون غير أولي فهو حتماً عدد أولي.

الموضوع:

تمرين إضافي: نفرض أن n عدد صحيح موجب وليكن $\varphi(n)$ دالة أويلر $\varphi(n), n\in\mathbb{Z}^+$

برهن أنه:

① إذا كان n فردياً $\Leftarrow$ فإن $\varphi(2n)=\varphi(n)$

② n زوجي $\Leftarrow$ فإن $\varphi(2n)=2\varphi(n)$

الحل: ① n فردي $\Leftarrow$ $d(2,n)=1$

$\Leftarrow$

$$\varphi(2n)=\varphi(2)\,\varphi(n)$$
$$=1\cdot\varphi(n)$$

② n زوجي $\Leftarrow$ $n=2^k\cdot m\ ;\ d(2^k,m)=1$

$$\varphi(n)=\varphi(2^k)\,\varphi(m)$$
$$=2^{k-1}(2-1)\,\varphi(m)=2^{k-1}\varphi(m)$$

$$\varphi(2n)=\varphi(2\cdot 2^{k+1}\cdot m)$$
$$=\varphi(2^{k+1}\cdot m)$$
$$=\varphi(2^{k+1})\,\varphi(m)$$
$$=2^k(2-1)\,\varphi(m)$$
$$=2^k\varphi(m)=2\cdot\underbrace{2^{k-1}\varphi(m)}_{\varphi(n)}$$
$$=2\varphi(n)$$

وهو المطلوب